Digital und sicher: Neue Wege für die Schulkommunikation

Studiengang: BSc in Informatik
Vertiefung: IT Security
Betreuer: Prof. Dr. Philipp Locher
Experte: Martin Arnold (AMCons GmbH)

Die Digitalisierung eröffnet Schulen neue Möglichkeiten für Kommunikation und Verwaltung. Gleichzeitig steigen die Anforderungen an den Schutz personenbezogener Daten von Kindern und Jugendlichen. Diese Arbeit zeigt, wie eine schulische Kommunikationslösung konsequent nach dem Prinzip „Privacy by Design“ entwickelt werden kann. Durch geeignete kryptografische Verfahren wird sichergestellt, dass selbst der Plattformbetreiber keinen Zugriff auf sensible Inhalte hat.

Aktuelle Lage

Zahlreiche bestehende Systeme adressieren zwar funktionale Anforderungen, missachten jedoch grundlegende Prinzipien des Datenschutzes. Häufig werden sensible Informationen lediglich auf Anwendungsebene geschützt, während der Plattformbetreiber technisch weiterhin uneingeschränkten Zugriff behält. Selbst bei verschlüsselter Übertragung sind Daten im Ruhezustand oftmals unzureichend abgesichert. Ein Datenleck kann schwerwiegende Folgen haben, nicht nur für betroffene Schüler und Schülerinnen, deren schulische und berufliche Laufbahn sowie Privatsphäre langfristig beeinträchtigt werden können, sondern auch für den Anbieter selbst, dessen Reputation erheblich leiden kann.

Ziele

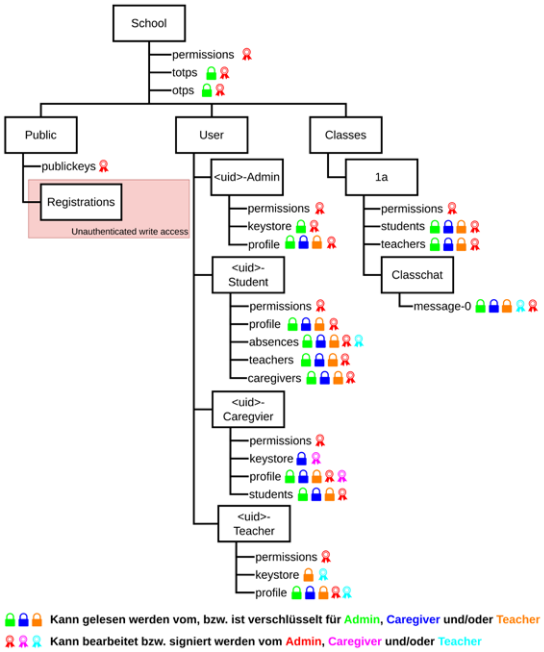
Ziel dieser Arbeit war die Konzeption und Umsetzung einer datenschutzkonformen Kommunikationslösung für den schulischen Kontext. Der Schutz sensibler Daten vor unbefugtem Zugriff, insbesondere durch den Plattformbetreiber, stand im Zentrum. Dabei wurden sichere 1:1- und Gruppenchats, die Kombination hoher Sicherheitsstandards mit benutzerfreundlicher Bedienung sowie eine klare, praktisch umsetzbare Spezifikation der Sicherheitsmechanismen angestrebt. Die Arbeit verfolgt einen durchgängig technischen Ansatz, der Datenschutz von Beginn an strukturell verankert. Besonderes Augenmerk galt der Modularität, insbesondere im Hinblick auf den Prototyp, um grundlegende kryptografische Mechanismen bei Bedarf flexibel austauschen zu können.

Nicolin Dora
nicolin.dora@protonmail.com

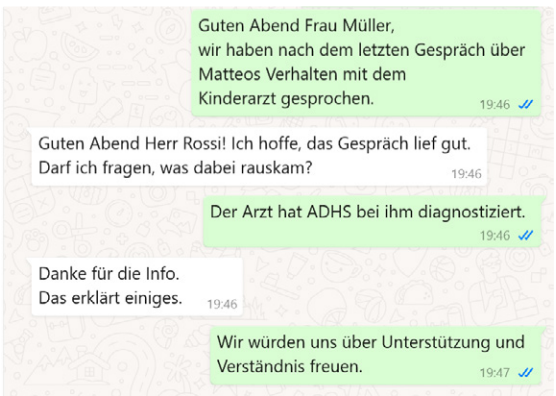
Ergebnisse

Kernresultat dieser Arbeit ist eine modulare, wiederverwendbare Spezifikation, die zeigt, wie sichere schulische Kommunikation ohne Zugriffsmöglichkeiten des Plattformbetreibers technisch realisiert werden kann. Um deren Praxistauglichkeit zu überprüfen, wurde ein technischer Prototyp entwickelt, der zentrale Funktionen exemplarisch umsetzt. Dabei kamen unter anderem clientseitige Verschlüsselung, kryptografische Zugriffskontrollen sowie sichere Backup-Mechanismen für Schlüsselmaterial zum Einsatz, alle erfolgreich implementiert und getestet. Die Ergebnisse zeigen, dass hohe Sicherheitsanforderungen mit praktikabler Umsetzung und guter Benutzererfahrung vereinbar sind.

Abidin Vejseli
abidin.vejseli@gmail.com



Übersicht der Ordnerstruktur und Zugriffsrechte in der Schulplattform



Beispielhafter WhatsApp-Chat zwischen einem Elternteil (grün) und einer Lehrperson (weiss)